Network Working Group
Internet-Draft
Updates: 2181 (if approved)
Intended status: Standards Track
Expires: 3 September 2026

K. Fujiwara
JPRS
W. Toorop
NLnet Labs

2 March 2026

Clarifications to the DNS Ranking Data
draft-fujiwara-dnsop-ranking-data-01

Abstract

This document obsoletes Section 5.4.1 (Ranking data) of RFC 2181, and specifies directives whereby the source of the data determines for what purposes it may be used.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

The DNS server assumed in Section 5.4.1 (Ranking data) of [RFC2181] is considered to be a model with a shared database described in Section 2.2 (Common configurations) of [RFC1035] that has both Authoritative server and Recursive Resolver functions. It is assumed that information obtained from zone files, zone transfers, and name resolution will be mixed together.

However, at the time of writing, this is no longer the practice of name servers and resolvers. Zone transfers transfer the same data from primaries to secondary servers without any modification. An authoritative name server function does not mix and return information obtained from name resolution.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Many of the specialized terms used in this document are defined in DNS Terminology [RFC9499].

3. Problem Statement

In the past, recursive resolvers would return data from referral responses, such as delegation information or glue, in the answer section of responses; however, modern recursive resolvers complete name resolution with an authoritative response from an authoritative server that has authority through delegation. However, there is no clear documentation of this.

"The Ranking Data" only indicates the priority among data, not its validity. Attacks using responses that do not correspond to queries and additional data that is not required have been considered and reported, so unnecessary data should be discarded.

[RFC1034] already describes resolver’s answer as follows.

"The ideal answer is one from a server authoritative for the query which either gives the required data or a name error. The data is passed back to the user and entered in the cache for future use if its TTL is greater than zero." (Quoted from RFC 1034, Section 5.3.3)

"The simplest mode for the client is recursive, since in this mode the name server acts in the role of a resolver and returns either an error or the answer, but never referrals." (Quoted from RFC 1034, Section 4.3.1)

Currently, responses from authoritative servers are considered to include authoritative name resolution results (NXDOMAIN, NODATA, the RRSet requested), non-authoritative delegation information, unnecessary data, and other types of errors, and each of these is considered to affect how resolvers handle the data. Therefore, directives on how to handle the data are needed.

4. Directives

1. Authoritative servers MUST NOT merge zone data. (zone data should be retrieved from a source (zone file, internal database, zone transfer)

2. Name resolution results (Answer section, or NXDOMAIN, NODATA) MUST be authoritative responses from authoritative servers that has authority through delegation.

3. Non-authoritative responses (referral/delegation responses) from authoritative servers MUST only be used to query the delegated authoritative server during the name resolution.

4. Names and IP addresses of the authoritative name servers for zones (such as the root zone) that are built-in or loaded from "hints" files, MUST only be used for priming a resolver for those zones [RFC9609].

5. Multi-function name server

Name servers with multiple functions will act as an Authoritative, Recursive Resolver (Full-Service Resolver), or Forwarder depending on the namespace to which the query name belongs, the server IP address, the "Recursion Desired" bit, etc. The data handled by each function MUST be separated.

5. Additional Considerations

[Further directives could be made, they may be DNS software implementation guidelines, which would be large in scale, so it is necessary to consider whether to proceed with them.]

* If a DNS server plays different roles for different namespaces (authoritative server, recursive resolver, forwarder), it MUST NOT merge DNS data for each role.

  For example, a recursive resolver that returns a fixed zone as a split-horizon DNS can be interpreted as acting as an authoritative server below a certain domain name, but as a recursive resolver otherwise.

* The Additional Section returned as the result of name resolution MUST be exactly the same as the Additional Section that came from the authoritative response from the authoritative server, or a separate authoritative response resulting from name resolution.

* Full-service resolvers SHOULD only accept the following data from authoritative servers:

  - NS and DS RRSets (+RRSIG) in the Authority Section of the delegation response and Glue A/AAAA in the Additional Section,

  - SOA RRs (+RRSIG) in the Authority Section of authoritative NXDOMAIN and NODATA responses in response to the query,

  - the Answer Section (+RRSIG) of the authoritative response in response to the query, and

  - any additional sections allowed by type (delegated domain name),

  and SHOULD NOT accept any other information.

6. IANA Considerations

This document requests no IANA actions.

7. Security Considerations

8. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/rfc/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, DOI 10.17487/RFC2181, July 1997, <https://www.rfc-editor.org/rfc/rfc2181>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/rfc/rfc9499>.

[RFC9609] Koch, P., Larson, M., and P. Hoffman, "Initializing a DNS Resolver with Priming Queries", BCP 209, RFC 9609, DOI 10.17487/RFC9609, February 2025, <https://www.rfc-editor.org/rfc/rfc9609>.

Authors' Addresses

Kazunori Fujiwara
Japan Registry Services Co., Ltd.
Japan
Email: fujiwara@jprs.co.jp

Willem Toorop
NLnet Labs
Science Park 400
1098 XH Amsterdam
Netherlands
Email: willem@nlnetlabs.nl